WHAT IS CLAIMED:

1. A system for performing penetration testing of a target computer network by installing a remote agent in the target computer network, the system comprising:

a local agent provided in a console and configured to receive and execute commands;

a user interface provided in the console and configured to send commands to and receive information from the local agent, process the information, and present the processed information;

a database configured to store the information received from the local agent;

a network interface connected to the local agent and configured to communicate via a network with the remote agent installed in the target computer network; and

security vulnerability exploitation modules for execution by the local agent and/or the remote agent.

2. The system of claim 1, wherein the user interface enables a user to select one of the modules and initiate execution of the selected module on either the local agent or the remote agent.

3. The system of claim 1, wherein the user interface provides a graphical representation of the target computer network.

4. A method for performing penetration testing of a target computer network, comprising:

installing a remote agent in the target computer network;

executing a command using a local agent provided in a console;

receiving information from the local agent in a user interface provided in the console;

presenting the information received from the local agent to a user;

storing the information received from the local agent in a database;

communicating via a network with the remote agent installed in the target computer network; and

providing security vulnerability exploitation modules for execution by the local agent and/or the remote agent.

5. The method of claim 4, further comprising:

selecting, using the user interface, one of the modules; and

initiating execution of the selected module on either the local agent or the remote agent.

6. The method of claim 4, further comprising providing a graphical representation of the target computer network using the user interface.

7. Computer code for performing penetration testing of a target computer network, the computer code comprising code for:

installing a remote agent in the target computer network;

executing a command using a local agent provided in a console;

receiving information from the local agent in a user interface provided in the console;

presenting the information received from the local agent to a user;

storing the information received from the local agent in a database;

communicating via a network with the remote agent installed in the target computer network; and

providing security vulnerability exploitation modules for execution by the local agent and/or the remote agent.

8. The computer code of claim 7, further comprising code for:

selecting, using the user interface, one of the modules; and

initiating execution of the selected module on either the local agent or the remote agent.

9. The computer code of claim 7, further comprising code for providing a graphical representation of the target computer network using the user interface.

10. An agent for use in a system for performing penetration testing of a target computer network, the agent comprising:

a proxy server configured to receive and execute system calls received via a network; and

a virtual machine configured to execute scripting language instructions received via the network.

11. The agent of claim 10, further comprising an execution engine configured to control the proxy server and the virtual machine, wherein the system calls and the scripting language instructions are routed to the proxy server and the virtual machine, respectively, by the execution engine.

12. The agent of claim 11, further comprising a remote procedure call module configured to receive commands from the network formatted in a remote procedure call protocol and pass the commands to the execution engine.

13. An agent for use in a system for performing penetration testing of a target computer network, the agent comprising:

a proxy server configured to receive and execute system calls received via a network;

a virtual machine configured to execute scripting language instructions received via the network;

a secure communication module configured to provide secure communication between the virtual machine and the network;

an execution engine configured to control the proxy server and the virtual machine, wherein the system calls and the scripting language instructions are routed to the proxy server and the virtual machine, respectively, by the execution engine;

a remote procedure call module configured to receive commands via the network formatted in a remote procedure call protocol and pass the commands to the execution engine; and

a second secure communication module configured to provide secure communication between the remote procedure call module and the network.

14. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module in a console having a user interface, the first module being configured to exploit a security vulnerability in a first target host of the target network;

installing a first remote agent in the first target host, the first remote agent being configured to communicate with the console and a second remote agent; and

executing a second module in the first remote agent, the second module being configured to exploit a security vulnerability in a second target host of the target network.

15. The method of claim 14, further comprising installing a second remote agent in the second target host of the target network, the second remote agent being configured to communicate with the first remote agent.

16. A system for performing penetration testing of a target network, comprising:

a console having a user interface;

a first module configured to execute in the console to exploit a security vulnerability in a first target host of the target network;

a first remote agent installed in the first target host, the first remote agent being configured to communicate with the console and a second remote agent; and

a second module configured to execute in the first remote agent to exploit a security vulnerability in a second target host of the target network.

17. The system of claim 16, further comprising a second remote agent installed in the second target host of the target network, the second remote agent being configured to communicate with the first remote agent.

18. Computer code for performing penetration testing of a target network, the computer code comprising code for:

executing a first module in a console having a user interface, the first module being configured to exploit a security vulnerability in a first target host of the target network;

installing a first remote agent in the first target host, the first remote agent being configured to communicate with the console and a second remote agent; and

executing a second module in the first remote agent, the second module being configured to exploit a security vulnerability in a second target host of the target network.

19. The computer code of claim 18, further comprising code for installing a second remote agent in the second target host of the target network, the second remote agent being configured to communicate with the first remote agent.

20. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

sending a system call to the first remote agent via a network; and

executing the system call in the first target host using a proxycall server of the first remote agent to exploit a security vulnerability of a second target host.

21. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing in the first remote agent a second module that generates a system call; and

executing the system call in the first target host to exploit a security vulnerability of a second target host.

22. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing a second module in the first remote agent that generates a system call;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending the system call generated by the second module to the second remote agent via a network; and

executing the system call in the second target host using a proxycall server of the second remote agent.

23. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending a system call to the first remote agent;

sending the system call from the first remote agent to the second remote agent; and

executing the system call in the second target host using a proxycall server of the second remote agent.

24. A method for performing penetration testing of a target network, comprising the steps of:

installing a first remote agent in the first target host, the first remote agent having a proxy server configured to receive and execute system calls;

executing in the first remote agent a system call received via a network;

installing a second remote agent in the first target host, the second remote agent having a proxy server configured to receive and execute system calls and a virtual machine configured to execute scripting language instructions; and

executing in the second remote agent a scripting language instruction or a system call, the system call being received via the network.

25. Computer code for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

sending a system call to the first remote agent via a network; and

executing the system call in the first target host using a proxycall server of the first remote agent to exploit a security vulnerability of a second target host.

26. Computer code for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing in the first remote agent a second module that generates a system call; and

executing the system call in the first target host to exploit a security vulnerability of a second target host.

27. Computer code for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing a second module in the first remote agent that generates a system call;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending the system call generated by the second module to the second remote agent via a network; and

executing the system call in the second target host using a proxycall server of the second remote agent.

28. Computer code for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending a system call to the first remote agent;

sending the system call from the first remote agent to the second remote agent; and

executing the system call in the second target host using a proxycall server of the second remote agent.

29. Computer code for performing penetration testing of a target network, the code comprising code for:

installing a first remote agent in the first target host, the first remote agent having a proxy server configured to receive and execute system calls;

executing in the first remote agent a system call received via a network;

installing a second remote agent in the first target host, the second remote agent having a proxy server configured to receive and execute system calls and a virtual machine configured to execute scripting language instructions; and

executing in the second remote agent a scripting language instruction or a system call, the system call being received via the network.